REMARKS

Please reconsider the claims in the application in view of the remarks below. Claims 1-30 remain pending in the present application.

Claim Rejection – 35 U.S.C. §112

Claims 1-30 stand rejected under 35 U.S.C. §112, first paragraph, allegedly because the specification does not provide enablement for "no link" between the client machine and authentication server. Applicants disagree. The specification thoroughly describes the mechanism in which a user is authenticated by the client machine and the authentication server without the client machine and the authentication server communicating during the authentication process. Further, the specification in paragraph [0022] specifically explains, "Accordingly, it can be seen that the present invention provides a computer system and method wherein a user is authenticated to both an authentication server and to a client machine, *but no link between the client machine and authentication server is needed*. Login information is provided from the client machine to the technician machine in an encrypted format that cannot be accessed by the technician machine. The technician machine communicates the encrypted login information to an authentication server, which decrypts the login information and provides it to the technician machine if the technician machine can authenticate itself to the authentication server. The invention is particularly useful in enabling field service technicians to access client computer systems from remote locations such as field offices, hotel rooms, airports and the like. However, other uses are possible" (emphasis added). From this explanation, a person of ordinary skill in the pertinent art would understand what is meant by "no link" and would be fully enabled to make and use the invention as claimed.

Nonetheless in this reply, that phrase is being deleted in order to further advance the prosecution of the present application and because the claims in the present application are unobvious even without that limitation as described below.

Instead, independent claims are being amended to recite, "no direct connection being needed between the client machine and the authentication server to authenticate the user's access to the client machine." Support for the amendment is found at least in paragraph [0022] of the originally submitted application. The Office Action concedes that the specification is enabling for no "direct connection." Accordingly, applicants believe that the claims as amended meet the requirements of section 112.

Claim Rejection – 35 U.S.C. §103

The Office Action rejected claims 1-30 under 35 U.S.C. §103(a) as allegedly being unpatentable over U.S. Patent Publication No. 2003/0217288 ("Guo et al.") in view of U.S. Patent Publication No. 2003/0208695 ("Soto et al."). While applicants disagree with the rejections set forth in the Office Action for the reasons explained below, applicants in this reply are amending independent claims 1, 10-12, 20-21, 28-30 to further clarify what is being claimed. Support for the amendment can be found at least in paragraph [0022] of the originally submitted specification.

Guo et al. as understood by applicant discloses a client computer that accesses web site hosted by affiliate server and renders a sign-in page to client computer. The affiliate server then redirects client to authentication server. The client follows the redirect to login.authsite.com, enters username and password that is known or accessible to the user, and is authenticated by the

authentication server. The authentication server redirects client back to web service at affiliate

server and the client follows the redirect to web service at affiliate server.

Soto et al. as understood by applicant discloses remotely accessing an external node.

Soto et al. in the cited passages (paragraphs [0053 - 0055]) refers to a remote access server

creating a local account on the remote access server using the same username and one-time

password and providing the one-time password to the user so that the user can log on to the

remote access server. Soto et al., however, fails to disclose, suggest or teach an encrypted login

and authentication information that is communicated to an authentication server, let alone

information that are not accessible by the user machine at the time of communicating that

information to the authentication server, and wherein no direct connection need to be established

between the client machine and the authentication server. Rather, Soto et al. appears to disclose

that the user directly uses the one-time password given to the user by the remote access server to

log on to the remote access server. That password is known to the user and accessible by the

user.

On the other hand, independent claims as amended in the present application recite, "the

encrypted login information and authentication information associated with the user being in an

encrypted format that cannot be accessed by the user machine when the user machine

communicates the encrypted login information and authentication information to the

authentication server... no direct connection being needed between the client machine and the

authentication server to authenticate the user's access to the client machine" Unlike the claims

in the present application, both Guo et al. and Soto et al. require that the user enter a specific

username and password accessible or known to the user and that client machine and the machine

that performs authentication (i.e., authentication server in Guo et al. and remote access server in

Soto et al.) communicate for authenticating the user. For example, while the Examiner cited

paragraph [0051] of Guo et al. refers to an encrypted ticket, that ticket is communicated directly

from the authentication server to the client machine (affiliate server). Without such login and

communication schemes between their client machines and authentication servers, Guo et al. and

Soto et al.'s authentication mechanism would not work.

Guo et al. and Soto et al., whether alone or in combination, thus do not render the claims

in the present application obvious. For at least the above reasons, independent claims and their

respective dependent claims by virtue of dependency in the present application are believed to be

unobvious over the cited references.

Applicants further disagree with the Examiner's allegation that Guo et al., discloses the

claimed elements of independent claims in the present application. For example, the Office

Action alleges that Guo et al. in paragraph [0047] discloses, "encrypting the login information at

the client machine and communicating the encrypted login information to the user machine."

That passage of Guo et al. describes that the authentication server provides a user with a user

interface page that accepts username/password, and validates the username/password entered by

the user. That passage plainly does not disclose or suggest that the client machine encrypts the

login information and communicates the encrypted login information to the user machine.

Applicants further dispute the Office Action's allegation that Guo et al.'s Figure 3

element 50, discloses, "communicating the encrypted login information and authentication

information associated with the user from the user machine to an authentication server."

Element 50 of Guo et al.'s Figure 3 specifies that "user enters username/password and the

username/password is posted to authentication server at login.authsite.com." User entering

username/password as Guo et al's Figure 3 element 50 explains, does not disclose or suggest a

user machine communicating the encrypted login information that was encrypted by the client machine to an authentication server.

Applicants also disagree with the Office Action's characterization that Guo et al.'s paragraphs [0039], [0040], [0049] and [0050] disclose, "decrypting the encrypted login information at the authentication server and communicating the decrypted login information to the user machine if the authentication information is acceptable to the authentication server." Those passages of Guo et al. describe PKI digital certificates and Guo et al.'s affiliate server decrypting the session key using its private key and decrypting the message content using the session key. Those passages do not disclose or suggest that the authentication server decrypts the encrypted login information and communicates the decrypted login information to the user machine.

Soto et al. does not make up for the above-described deficiencies of Guo et al. Therefore, for at least those reasons, independent claims in the present application and their respective dependent claims, at least by virtue of their dependencies, are unobvious over Guo et al. and Soto et al.

This communication is believed to be fully responsive to the Office Action and every effort has been made to place the application in condition for allowance. A favorable Office Action is hereby earnestly solicited. If the Examiner believes a telephone conference might expedite prosecution of this case, it is respectfully requested that the Examiner call applicant's attorney at (516) 742-4343.

Respectfully submitted,

Eunhee Park
Registration No.: 42,976

Scully, Scott, Murphy & Presser, P.C.
400 Garden City Plaza, Suite 300
Garden City, N.Y. 11530
(516) 742-4343

EP:vh

I:\IBM\1545\16874\amend\16874.am5.doc